

**WOMBLE  
CARLYLE  
SANDRIDGE  
& RICE**  
A PROFESSIONAL LIMITED  
LIABILITY COMPANY

1401 Eye Street, NW  
Seventh Floor  
Washington, DC 20005

Telephone: (202) 467-6900  
Fax: (202) 467-6910  
www.wcsr.com

Jennifer M. Kashatus  
Attorney  
Direct Dial: (202) 857-4506  
Direct Fax: (202) 261-0006  
E-mail: JKashatus@wcsr.com

March 3, 2008

**VIA ECFS**

Marlene Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, SW  
Washington, D.C. 20005

Re: Unipoint Enhanced Services Inc., FCC Filer ID 825974, EB Docket No. 06-36

Dear Ms. Dortch:

Unipoint Enhanced Services Inc. through its undersigned counsel and in accordance with the Commission's *Public Notice* DA 08-171 in the above-referenced docket, respectfully submits its annual Customer Proprietary Network Information Certification and accompanying statement.

Please contact me if you have any questions regarding this filing.

Respectfully submitted,

**WOMBLE CARLYLE SANDRIDGE & RICE**  
*A Professional Limited Liability Company*



Jennifer M. Kashatus

cc: Best Copy & Printing (via email)

Annual 47 C.F.R. § 64.5009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: February 28, 2008

Name of company covered by this certification: Unipoint Enhanced Services Inc.

Form 499 Filer ID: 825974

Name of signatory: Mike Holloway

Title of signatory: CEO and President

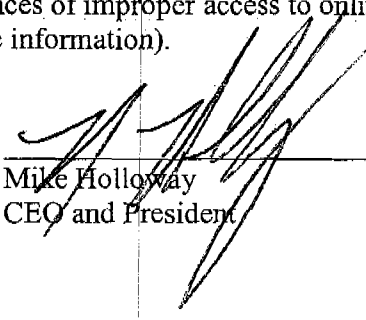
I, Mike Holloway, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2007 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

  
\_\_\_\_\_  
Mike Holloway  
CEO and President

**STATEMENT REGARDING UNIPOINT ENHANCED SERVICES, INC.  
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)  
OPERATING PROCEDURES**

**February 29, 2008**

UniPoint Enhanced Services("UniPoint" or "Company") provides this statement pursuant to 47 C.F.R. § 64.2009(e) to explain how UniPoint's operating procedures were designed to ensure compliance with the Federal Communications Commission's ("Commission") CPNI rules for the period from December 8, 2007, to December 31, 2007.

**Certification**

UniPoint requires an officer of the Company to sign and file with the Commission a compliance certification on an annual basis. The certification is based on the personal knowledge of the certifying officer, acquired through personal information and inquiry, that UniPoint has established operating procedures designed to ensure compliance with the Commission's CPNI rules. UniPoint's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

**Customer Approval to Use, Disclose, or Permit Access to CPNI**

UniPoint does not use, disclose, or permit access to its customers' CPNI except as such use, disclosure, or access is permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Accordingly, the customer notice and associated record-keeping requirements of the Commission's CPNI rules are not applicable. Should UniPoint change its policies such that the use, disclosure, or permitted access to CPNI requires customer approval, appropriate customer notice, record-keeping, and FCC notification practices will be implemented.

Consistent with the Commission's rules, although UniPoint does not necessarily engage in each of the following activities, UniPoint's policies permit it to use, disclose, or permit access to CPNI without customer approval for the purpose of:

- providing or marketing service offerings among the categories of service to which the customer already subscribes without customer approval;
- provisioning customer premises information (CPE) and information service(s);
- marketing services such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features;

- protecting the rights or property of the providers, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; and
- as otherwise permitted in Section 222 of the Communications Act of 1934, as amended.

### **Notice of CPNI Rights**

As explained above, UniPoint does not use, disclose, or permit access to its customers' CPNI except as permitted without customer approval, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Therefore, UniPoint is not required to provide customer notice regarding CPNI rights as prescribed in the Commission's rules. Should UniPoint change its policies such that customer notice is required, such notice will be provided.

### **Record Retention for Marketing Campaigns**

To the extent that UniPoint uses CPNI for marketing reasons, UniPoint maintains records of sales and marketing campaigns that use CPNI. Records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. UniPoint maintains such records for at least one year.

### **Reporting Opt Out Failures**

UniPoint's policy is to not use, disclose, or permit access to its customers' CPNI without customer approval except as permitted under the Commission's rules or as otherwise provided in Section 222 of the Communications Act of 1934, as amended. Should UniPoint change its policies and seek customer approval to use, disclose, or permit access to CPNI, UniPoint will provide written notice of opt-out failures to the Commission within five business days as specified in the Commission's rules.

### **Supervisory Review Process**

UniPoint takes the privacy and security of CPNI seriously. UniPoint has a supervisory review process that governs its use of CPNI. As a general matter, employees must receive permission from their supervisors or other authorized personnel before using or disclosing CPNI for sales or marketing purposes.

### **General Privacy and Security Measures**

UniPoint has implemented numerous controls to ensure compliance with the FCC's CPNI rules. For example CPNI information is not generally given via verbal or telephone request. CPNI information such as customer call detail records are made available as secure online portal which requires customers to enter an authorized account number, username, and password.

### **Customer Authentication Procedures**

UniPoint has established procedures that require proper authentication prior to disclosing

CPNI based on customer-initiated telephone contacts, and online. UniPoint does not disclose call detail information over the telephone in response to customer-initiated telephone contacts unless the customer provides a previously-established Personal Identification Number ("PIN") or password. If UniPoint cannot authenticate a customer through the PIN/password process, UniPoint either will disclose call detail information only by calling the customer at the telephone number of record or by transmitting the information to the email address(es) of record. Online account access to CPNI is permitted only with an account number, username, and password.

#### **Employee Discipline Program**

UniPoint has a disciplinary process in place to address noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated UniPoint's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

#### **Notice of Security Breaches**

UniPoint notifies law enforcement as soon as practicable, but in no event later than seven (7) business days after a reasonable determination has been made that a breach of its customer's CPNI has occurred. The notice process conforms to procedures established by the Commission and is otherwise in accordance with 47 C.F.R. § 64.2011.

UniPoint strives to notify customers of the breach no sooner than the eighth business day following completion of the notice to law enforcement unless directed by the U.S. Secret Service or the FBI not to disclose or notify customers. UniPoint respects any agency request that UniPoint not to disclose the breach for an initial period of up to 30 days, which may be extended further by the agency. The requesting agency must provide its direction in writing, as well as any notice that delay is no longer required.

#### **Record keeping of Unauthorized Disclosures of CPNI, Customer Complaints, and Actions Taken Against Pretexting**

A record of CPNI security breaches, notifications made to law enforcement, and notifications made to customers is maintained for at least two years.

Customer complaints concerning the unauthorized release of CPNI are reported and investigated internally, and are broken out by category of complaint (e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized). A summary of all such complaints in the prior year is included along with the annual certification to the Commission.

A record of any actions taken by UniPoint against data brokers is maintained and an explanation of such actions included with the annual certification to the Commission, including any information UniPoint has with respect to the processes pretexters are using to attempt to access CPNI.